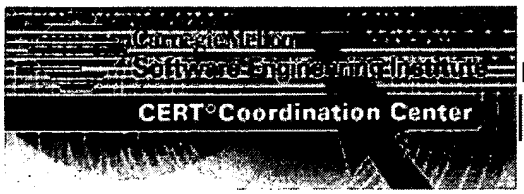

Options

Advisories

US-CERT Vulnerability Notes Database

Incident Notes

Current Activity

Related

Summaries

Tech Tips

AirCERT

Employment Opportunities

more links

CERT Statistics

Vulnerability Disclosure Policy

CERT Knowledgebase

System Administrator courses

CSIRT courses

Other Sources of Security Information

Channels

Message

CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks

Original issue date: September 19, 1996
Last revised: November 29, 2000
Updated vendor information for the Linux kernel.

A complete revision history is at the end of this file. **This advisory supersedes the IP spoofing portion of CA-95.01.**

Two "underground magazines" have recently published code to conduct denial-of-service attacks by creating TCP "half-open" connections. This code is actively being used to attack sites connected to the Internet. There is, as yet, no complete solution for this problem, but there are steps that can be taken to lessen its impact. Although discovering the origin of the attack is difficult, it is possible to do; we have received reports of attack origins being identified.

Any system connected to the Internet and providing TCP-based network services (such as a Web server, FTP server, or mail server) is potentially subject to this attack. Note that in addition to attacks launched at specific hosts, these attacks could also be launched against your routers or other network server systems if these hosts enable (or turn on) other TCP services (e.g., echo). The consequences of the attack may vary depending on the system; however, the attack itself is fundamental to the TCP protocol used by all systems.

If you are an Internet service provider, please pay particular attention to Section III and Appendix A, which describes step we urge you to take to lessen the effects of these attacks. If you are the customer of an Internet service provider, please encourage your provider to take these steps.

This advisory provides a brief outline of the problem and a partial solution. We will update this advisory as we receive new information. If the change in information warrants, we may post an updated advisory on comp.security.announce and redistribute an update to our cert-advisory mailing list. As always, the latest information is available at the URLs listed at the end of this advisory.

I. Description

When a system (called the client) attempts to establish a TCP connection to a system providing a service (the server), the client and server exchange a set sequence of messages. This connection technique applies to all TCP connections--telnet, Web, email, etc.

The client system begins by sending a SYN message to the server. The server then acknowledges the SYN message by sending SYN-ACK message to the client. The client

then finishes establishing the connection by responding with an ACK message. The connection between the client and the server is then open, and the service-specific data can be exchanged between the client and the server. Here is a view of this message flow:

```
Client                  Server
  ------                  ------
  SYN------------------->

     <--------------------SYN-ACK

  ACK------------------->

       Client and server can now
       send service-specific data
```

The potential for abuse arises at the point where the server system has sent an acknowledgment (SYN-ACK) back to client but has not yet received the ACK message. This is what we mean by half-open connection. The server has built in its system memory a data structure describing all pending connections. This data structure is of finite size, and it can be made to overflow by intentionally creating too many partially-open connections.

Creating half-open connections is easily accomplished with IP spoofing. The attacking system sends SYN messages to the victim server system; these appear to be legitimate but in fact reference a client system that is unable to respond to the SYN-ACK messages. This means that the final ACK message will never be sent to the victim server system.

The half-open connections data structure on the victim server system will eventually fill; then the system will be unable to accept any new incoming connections until the table is emptied out. Normally there is a timeout associated with a pending connection, so the half-open connections will eventually expire and the victim server system will recover. However, the attacking system can simply continue sending IP-spoofed packets requesting new connections faster than the victim system can expire the pending connections.

In most cases, the victim of such an attack will have difficulty in accepting any new incoming network connection. In these cases, the attack does not affect existing incoming connections nor the ability to originate outgoing network connections.

However, in some cases, the system may exhaust memory, crash, or be rendered otherwise inoperative.

The location of the attacking system is obscured because the source addresses in the SYN packets are often implausible. When the packet arrives at the victim server system, there is no way to determine its true source. Since the network forwards packets based on destination address, the only way to validate the source of a packet is to use input source filtering (see Appendix A).

II. Impact

Systems providing TCP-based services to the Internet community may be unable to provide those services while under attack and for some time after the attack ceases. The service itself is not harmed by the attack; usually only the ability to provide the service is impaired. In some cases, the system may exhaust memory, crash, or be rendered otherwise inoperative.

III. Solution

There is, as yet, no generally accepted solution to this problem with the current IP protocol technology. However, proper router configuration can reduce the likelihood that your site

will be the source of one of these attacks.

Appendix A contains details about how to filter packets to reduce the number of IP-spoofed packets entering and exiting your network. It also contains a list of vendors that have reported support for this type of filtering.

NOTE to Internet Service Providers:

We STRONGLY urge you to install these filters in your routers to protect your customers against this type of an attack. Although these filters do not directly protect your customers from attack, the filters do prevent attacks from originating at the sites of any of your customers. We are aware of the ramifications of these filters on some current Mobile IP schemes and are seeking a position statement from the appropriate organizations.

NOTE to customers of Internet service providers:

We STRONGLY recommend that you contact your service provider to verify that the necessary filters are in place to protect your network.

Many networking experts are working together to devise improvements to existing IP implementations to "harden" kernels to this type of attack. When these improvements become available, we suggest that you install them on all your systems as soon as possible. This advisory will be updated to reflect changes made by the vendor

IV. Detecting an Attack

Users of the attacked server system may notice nothing unusual since the IP-spoofed connection requests may not load the system noticeably. The system is still able to establish outgoing connections. The problem will most likely be noticed by client systems attempting to access one of the services on the victim system.

To verify that this attack is occurring, check the state of the server system's network traffic. For example, on SunOS this may be done by the command:

```
netstat -a -f inet
```

Note that use of the above command depends on the OS version, for example for a FreeBSD system use

```
netstat -s |grep "listenqueue overflows"
```

Too many connections in the state "SYN_RECEIVED" could indicate that the system is being attacked.

Appendix A - Reducing IP Spoofed Packets

1. Filtering Information

With the current IP protocol technology, it is impossible to eliminate IP-spoofed packets. However, you can take steps to reduce the number of IP-spoofed packets entering and exiting your network.

Currently, the best method is to install a filtering router that restricts the input to your

external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network. In addition, you should filter outgoing packets that have a source address different from your internal network to prevent a source IP spoofing attack from originating from your site.

The combination of these two filters would prevent outside attackers from sending you packets pretending to be from your internal network. It would also prevent packets originating within your network from pretending to be from outside your network. These filters will *not* stop all TCP SYN attacks, since outside attackers can spoof packets from *any* outside network, and internal attackers can still send attacks spoofing internal addresses.

We STRONGLY urge Internet service providers to install these filters in your routers.

In addition, we STRONGLY recommend customers of Internet service providers to contact your service provider to verify that the necessary filters are in place to protect your network.

2. Vendor Information

The following vendor(s) have reported support for the type of filtering we recommend and provided pointers to additional information that describes how to configure your router. If we hear from other vendors, we will add their information to the "Updates" section at the end of this advisory.

If you need more information about your router or about firewalls, please contact your vendor directly.

Cisco

Refer to the section entitled "ISP Security Advisory" on http://www.cisco.com for an up-to-date explanation of how to address TCP SYN flooding on a Cisco router.

NOTE to vendors:

If you are a router vendor who has information on router capabilities and configuration examples and you are not represented in this list, please contact the CERT Coordination Center at the addresses given in the Contact Information section below. We will update the advisory after we hear from you.

3. Alternative for routers that do not support filtering on the inbound side

If your vendor's router does not support filtering on the inbound side of the interface or if there will be a delay in incorporating the feature into your system, you may filter the spoofed IP packets by using a second router between your external interface and your outside connection. Configure this router to block, on the outgoing interface connected to your original router, all packets that have a source address in your internal network. For this purpose, you can use a filtering router or a UNIX system with two interfaces that supports packet filtering.

Note: Disabling source routing at the router does not protect you from this attack, but it is still good security practice to follow.

On the input to your external interface, that is coming from the Internet to your network, you should block packets with the following addresses:

- Broadcast Networks: The addresses to block here are network 0 (the all zeros broadcast address) and network 255.255.255.255 (the all ones broadcast network).
- Your local network(s): These are your network addresses

- Reserved private network numbers: The following networks are defined as reserved private networks, and no traffic should ever be received from or transmitted to these networks through a router:

```
10.0.0.0     - 10.255.255.255    10/8           (reserved)
127.0.0.0    - 127.255.255.255   127/8          (loopback)
172.16.0.0   - 172.31.255.255    172.16/12      (reserved)
192.168.0.0 - 192.168.255.255    192.168/16     (reserved)
```

The CERT Coordination Center staff thanks the team members of NASIRC for contributing much of the text for this advisory and thanks the many experts who are devoting time to addressing the problem and who provided input to this advisory.

UPDATES

3COM

Please refer to the "Network Security Advisory" for a thorough discussion of how to address TCP SYN flooding attacks on a 3Com router:

http://www.3com.com/

Berkeley Software Design, Inc.

BSDI has patches available.

PATCH

K210-021 (ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/K210-021)

md5 checksum: c386e72f41d0e409d91b493631e364dd K210-021

This patch adds two networking features that can help defeat and detect some types of denial of service attacks.

This patch requires U210-025 which provides new copies of *sysctl(8)* and *netstat(1)* for configuration and monitoring of these new features.

PATCH

K210-022 (ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/K210-22)

md5 checksum: 9ec62b5e9cc424b9b42089504256d926 K210-022

This patch adds a TCP SYN cache which reduces and/or eliminates the effects of SYN-type

denial of service attacks such as those discussed in CERT advisory CA 96.21.

PATCH

U210-025 (ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/U210-025)

md5 checksum: d2ee01238ab6040e9b7a1bd2c3bf1016 U210-025

This patch should be installed in conjunction with IP source address check and IP fragmentation queue limit patch (K210-021) and SYN flooding patch (K210-022).

Additional details about these patches are available from

http://www.bsdi.com
ftp://ftp.bsdi.com

Hewlett-Packard Company

HPSBUX9704-060

Description: SYN Flooding Security Vulnerability in HP-UX

HEWLETT-PACKARD SECURITY BULLETIN: #00060

Security Bulletins are available from the HP Electronic Support Center via electronic mail.

User your browser to get to the HP Electronic Support Center page at:

http://us-support.external.hp.com
(for US, Canada, Asia-Pacific, & Latin-America)

http://europe-support.external.hp.com
(for Europe)

IBM Corporation

Any system that is connected to a TCP/IP-based network (Internet or intranet) and offers TCP-based services is vulnerable to the SYN flood attack. The attack does not distinguish between operating systems, software version levels, or hardware platforms; all systems are vulnerable. IBM has released AIX operating system fixes for the SYN flood vulnerability.

NOTE: If you are using the IBM Internet Connection Secured Network Gateway (SNG) firewall software, you must also apply the fixes listed in the next section.

The following Automated Program Analysis Reports (APARs) for IBM AIX are now available to address the SYN flood attack:

AIX 3.2.5

No APAR available; upgrade to AIX 4.x recommended

AIX 4.1.x

APAR - IX62476

AIX 4.2.x

APAR - IX62428

Fixes for IBM SNG Firewall

The following Automated Program Analysis Reports (APARs) for the IBM Internet Connection Secured Network Gateway firewall product are now available to address the SYN flood and "Ping o' Death" attacks:

NOTE: The fixes in this section should ONLY be applied to systems running the IBM Internet Connection Secured Network Gateway (SNG) firewall software. They should be applied IN ADDITION TO the IBM AIX fixes listed in the previous section.

IBM SNG V2.1

APAR - IR33376 PTF UR46673

IBM SNG V2.2

APAR - IR33484 PTF UR46641

Obtaining Fixes

IBM AIX APARs may be ordered using Electronic Fix Distribution (via the FixDist program), or from the IBM Support Center. For more information on FixDist, and to obtain fixes via the Internet, please reference

http://service.software.ibm.com/aixsupport/

or send electronic mail to "aixserv@austin.ibm.com " with the word "FixDist" in the "Subject:" line.

Linux

A patch for version 2.0.29 of the linux kernel source is available from:

http://www.kernel.org/pub/linux/kernel/v2.0/patch-2.0.30.gz

The patch allows tcp/ip processing to continue as normal, until the queue gets close to full. Then, instead of just sending the synack back, it sends a syn cookie back, and waits for a response to IT before sending the synack. When it sends the cookie, it clears the syn from the queue, so while under attack, the queue will never fill up. Cookies expire shortly after they are sent. Basically this prevents people from filling up the queue completely. No one flooding from a spoof will be able to reply to the cookie, so nothing can be overloaded. And if they aren't flooding from a spoof, they would be getting a cookie they would have to respond to, and would have a hard time responding to all the cookies and continuing the flood.

Livingston Enterprises, Inc.

Refer to the following Applications Note for more information on configuring a Livingston

IRX or PortMaster to help block outgoing SYN attacks from an ISP's users:

ftp://ftp.livingston.com/pub/le/doc/notes/filters.syn-attack

Silicon Graphics, Inc.

Updated Silicon Graphics information concerning SYN attacks can be found in SGI Security Advisory, "IRIX IP Spoofing/TCP Sequence Attack Update," 19961202-01-PX, issued on August 6, 1998.

Patches are available via anonymous FTP and your service/support provider.

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectfully.

For subscribing to the wiretap mailing list and other SGI security related information, please refer to the Silicon Graphics Security Headquarters website located at:

http://www.sgi.com/Support/security

Sun Microsystems, Inc.

Sun published a bulletin on October 9, 1996--Sun security bulletin number 00136. Sun Security Bulletins are available via the security-alert@sun.com alias and on SunSolve.

Note: Advisories from vendors listed in this section can also be found at ftp://ftp.cert.org/pub/vendors/

This document is available from: http://www.cert.org/advisories/CA-1996-21.html

---

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
Nov. 29, 2000  Updated vendor information for the Linux kernel.
Aug. 24, 1998  Updated vendor information for Silicon Graphics, Inc.
Sep, 24, 1997  Updated copyright statement
July 18, 1997  Updates - added information
May  08, 1997  Updates - updated vendor information for Hewlett-Packard.
Jan. 02, 1997  Updates - added or modified vendor information for SGI,
               Livingston, HP, 3COM.
Dec. 19, 1996  Updates - corrected Sun Microsystems security-alert email
               address.
Dec. 10, 1996  Appendix A, #3 - corrected next to last reserved private
               network number entry.
Dec. 09, 1996  Updates - added IBM patch information.
Nov. 12, 1996  Introduction, paragraph 2 - added some clarification.
Oct. 10, 1996  Updates - added a pointer to Sun Microsystems advisory.
               added a pointer to the CERT /pub/vendors directory.
Oct. 08, 1996  Appendix A, #3 - revised the last item, reserved private
               network numbers
               Updates - added BSDI patch information.
Oct. 07, 1996  Updates - added a pointer to Silicon Graphics advisory.
Sep. 24, 1996  Modified the supersession statement.
```